(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
14 mars 2002 (14.03.2002)

PCT

(10) Numéro de publication internationale
WO 02/21436 A1

(51) Classification internationale des brevets[7] : G06K 19/08, G07F 7/08, G06K 19/07, B42D 15/10, G07C 9/00

(21) Numéro de la demande internationale : PCT/FR00/02462

(22) Date de dépôt international : 7 septembre 2000 (07.09.2000)

(25) Langue de dépôt : français

(26) Langue de publication : français

(71) Déposant et
(72) Inventeur : DESERT, Michel [FR/FR]; 4, rue du Maréchal Foch, F-78354 Jouy en Josas (FR).

(74) Mandataire : LAGET, Jean-Loup; Cabinet Loyer, 78, avenue Raymond Poincaré, F-75116 Paris (FR).

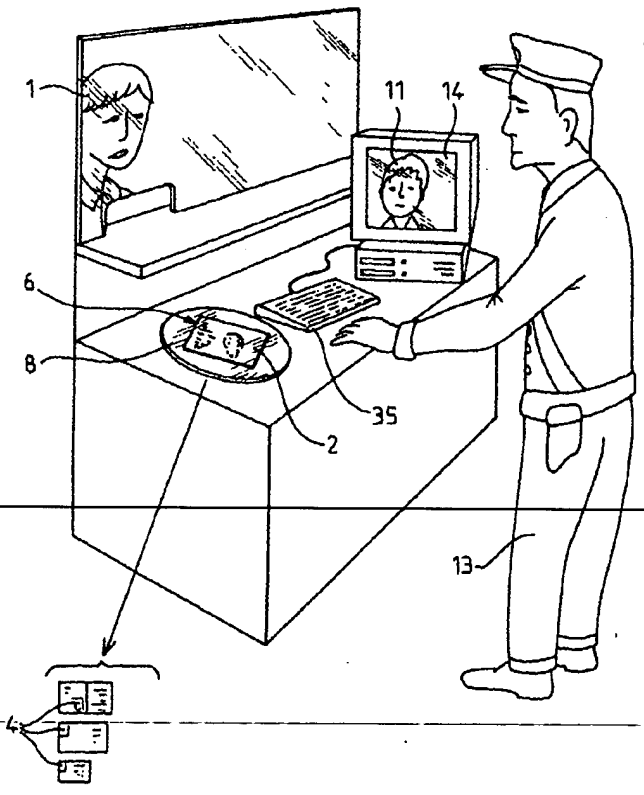
(81) États désignés *(national)* : AE, AL, AU, AZ, BA, BB, BG, BR, CA, CN, CR, CU, CZ, DM, EE, GD, GE, HR, HU, ID, IL, IN, IS, JP, KE, KR, LC, LK, LR, LT, LV, MA, MD, MK, MN, MX, NO, NZ, PL, RO, SD, SG, SI, SK, SL, TR, TT, US, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR DETECTING FORGERY OF A DOCUMENT DELIVERED TO AN INDIVIDUAL

(54) Titre : PROCEDE ET SYSTEME DE DETECTION D'UNE FALSIFICATION D'UN DOCUMENT DELIVRE A UNE PERSONNE PHYSIQUE



(57) Abstract: The invention concerns a method and a system, wherein the document (2) delivered to said individual (1) further comprises at least a contact or non-contact memory chip (6) with contact or non-contact read/write, or contact or non-contact chip (6), said at least one contact or non-contact chip (6) comprising a storage (6), the data contained in said storage (7) of said at least one contact or non-contact chip (6) being capable of being read and/or written by a contact or non-contact chip reader (8).

(57) Abrégé : Le document (2) délivré à ladite personne physique (1) comporte en outre au moins une puce avec ou sans contacts (6) à lecture/écriture avec ou sans contacts, ou puce avec ou sans contacts (6), ladite au moins une puce avec ou sans contacts (6) comportant une mémoire (7), les données contenues dans ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) pouvant être lues et/ou écrites par un lecteur (8) de puce avec ou sans contacts.

WO 02/21436 A1

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE ET SYSTEME DE DETECTION D'UNE FALSIFICATION D'UN DOCUMENT DELIVRE A UNE PERSONNE PHYSIQUE

La présente invention concerne les documents délivrés à des personnes physiques, et plus particulièrement, un document intégrant une puce à mémoire à lecture et écriture et/ou à microprocesseur avec ou sans contacts pour en détecter la falsification, ainsi que l'utilisation d'un document d'identité de ce type pour contrôler l'identité d'une personne physique.

Les documents d'identité sont connus depuis plusieurs siècles, et ils ont connu une évolution en complexité et en sophistication parallèle à celle de la technique, afin de limiter autant que faire se peut la réalisation de faux documents d'identité ou la falsification de documents d'identité authentiques.

Toutefois, la démocratisation de ces mêmes progrès de la technique permet aux faussaires de contourner, avec un certain retard, les obstacles technologiques mis en place par les autorités pour rendre aussi difficile que possible la réalisation de ces faux documents.

Il existe donc une course permanente entre, d'une part, l'amélioration des techniques d'authentification des documents d'identité, et d'autre part, l'utilisation de ces mêmes techniques et/ou de techniques approchantes pour contrefaire ou falsifier ces mêmes documents.

Les documents d'identité actuels se présentent sous diverses formes et sont réalisés sur divers supports, tels que : livrets papier pour les passeports, feuille de papier unique, autocollante ou non, pour les visas, supports papier de diverses épaisseurs, cartonnés ou non, insérés dans un matériau plastique transparent ou non, comme cartes d'identité nationales, permis de conduire et/ou de séjour, cartes grises, etc. La plupart de ces documents d'identité actuels comportent une photographie du détendeur du document. Toutefois, le remplacement de cette photographie ne pose guère de problème à un faussaire expérimenté. Pour pallier cet inconvénient, depuis

un certain nombre d'années, un film de sécurité autocollant et transparent est apposé sur certains documents d'identité pour compliquer la tâche d'un contrefacteur éventuel, mais il existera dans un proche avenir des techniques permettant de venir à bout de cet obstacle.

Plus récemment, des hologrammes ont été ajoutés aux documents d'identité pour en rendre plus ardue la falsification, du fait que la production des hologrammes requiert la maîtrise d'une technologie avancée. Toutefois, la démocratisation de cette technologie permet depuis peu aux faussaires de trouver sur le marché des hologrammes pouvant, en faisant illusion, permettre la réalisation approximative de documents d'identité, trompant ainsi les personnes non expérimentées.

De même, un fil métallique ou plastique a été ajouté dans l'épaisseur du papier de certains documents d'identité pour en rendre la falsification plus difficile. A nouveau, cette technique est, de nos jours, à la portée des faussaires expérimentés.

En tout état de cause, si ces divers obstacles peuvent avoir une certaine efficacité en ce qui concerne la réalisation de toutes pièces d'un faux document d'identité, ils sont beaucoup moins efficaces en ce qui concerne la falsification d'un document d'identité authentique existant. En effet, il est en général plus facile comparativement de falsifier, sur un document d'identité authentique d'une personne physique, les informations propres à la personne physique telles que la photographie, la taille ou une empreinte digitale de cette personne physique, que de créer ex-nihilo un faux document d'identité avec de fausses informations, et incluant ces diverses technologies.

Compte-tenu du fait que les informations propres à la personne physique, telle que la photographie, la taille ou une empreinte digitale, sont encore à l'heure actuelle fixées sur support papier, il est toujours possible à un faussaire de falsifier ces informations par effaçage ou grattage, suivi d'une réinscription à l'aide d'encres appropriées.

Dans l'état actuel de la technique, la seule parade fiable réside donc dans la duplication des informations propres à la personne physique lors de la fabrication du document d'identité, de façon à permettre la comparaison des informations telles qu'elles apparaissent sur le document d'identité à

celles qui y figuraient à l'origine, de façon à pouvoir détecter toute falsification.

L'approche venant naturellement à l'esprit consisterait à stocker ces informations dans un système informatique qui serait interrogé à chaque vérification d'identité. Toutefois, pour appliquer ce système à l'échelle d'un état ou d'un groupement d'états tel que l'Europe ou les Etats-Unis, ce système nécessiterait une infrastructure très lourde en réseaux de communication et en ordinateurs centraux devant stocker des centaines de millions de données individuelles, avec les risques de défaillance et d'indisponibilité inhérents à toute structure de cette taille. De plus, des législations nationales ou internationales peuvent faire obstacle à la mise en place de tels dispositifs.

En outre, dans l'état actuel de la technique, une telle solution serait difficile à mettre en œuvre dans des brigades mobiles, telles que celles des polices des frontières, des gendarmeries, des douanes, etc., pour lesquelles une liaison fiable avec un site informatique central, nécessairement par voie hertzienne, serait problématique, en particulier en raison des difficultés inhérentes à ce type de transmission.

En conséquence, il existe donc un besoin pour un procédé et un système permettant de contrôler l'authenticité d'un document d'identité, c'est-à-dire, de contrôler la véracité des informations, propres à la personne physique, apparaissant sur le document, et permettant ainsi de contrôler l'identité de cette personne, sans nécessiter d'infrastructure lourde, c'est-à-dire, seulement à l'aide du document d'identité et d'un matériel léger, portable ou non.

La présente invention a donc pour objet un procédé de détection de falsification d'un document délivré à une personne physique, ledit document comportant au moins une photographie conventionnelle permettant d'identifier ladite personne physique, et/ou au moins un numéro de document inscrit permettant d'identifier ledit document de façon unique, et/ou le nom, et éventuellement les prénoms, et/ou la date de naissance et/ou le lieu de naissance de la personne physique et/ou une ou plusieurs données biométriques et/ou anthropométriques inscrites concernant ladite personne physique, et qui a pour caractéristique le fait

que ledit document délivré à ladite personne physique comporte en outre au moins une puce à lecture/écriture avec ou sans contacts, ou puce avec ou sans contacts, ladite au moins une puce avec ou sans contacts comportant une mémoire, les données contenues dans ladite mémoire de ladite au moins une puce avec ou sans contacts pouvant être lues et/ou écrites par un lecteur de puce avec ou sans contacts.

De préférence, ladite puce avec ou sans contacts peut comporter en outre au moins un microprocesseur et/ou au moins un microcontrôleur.

Avantageusement, dans le procédé de l'invention, ladite mémoire de ladite au moins une puce avec ou sans contacts dudit document peut en outre stocker une donnée d'identification non modifiable identifiant de façon unique ladite puce avec ou sans contacts. Cette donnée non modifiable dans la mémoire peut alors être inscrite sous une forme appropriée sur ledit document, et ledit document peut être déterminé comme étant falsifié si, après relecture de ladite donnée depuis ladite mémoire de ladite puce avec ou sans contacts par ledit lecteur, ladite donnée ainsi relue diffère de ladite donnée inscrite sur ledit document.

De préférence, lesdites données contenues dans ladite mémoire de ladite au moins une puce avec ou sans contacts dudit document sont protégées contre toute modification postérieure à l'enregistrement initial desdites données.

Egalement, dans le procédé de l'invention, une ou plusieurs photographies sous forme numérique de ladite personne physique peuvent être en outre stockées dans la mémoire de ladite au moins une puce avec ou sans contacts dudit document.

Ledit document peut comporter en outre une ou plusieurs photographies conventionnelles de ladite personne physique, et ledit document peut alors être déterminé comme étant falsifié si, après relecture desdites une ou plusieurs photographies sous forme numérique depuis ladite mémoire de ladite au moins une puce avec ou sans contacts par ledit lecteur, au moins une photographie sous forme numérique ainsi relue diffère de la photographie conventionnelle correspondante sur ledit document. De plus, l'identité de ladite personne physique peut alors être déterminée comme étant falsifiée si, après relecture desdites une ou plusieurs photographies

sous forme numérique depuis ladite mémoire de ladite au moins une puce sans contact par ledit lecteur, au moins une photographie sous forme numérique ainsi relue ne correspond pas à ladite personne physique.

En outre, dans le procédé de l'invention, au moins un numéro de document peut être inscrit sur ledit document, et ladite mémoire de ladite au moins une puce avec ou sans contacts dudit document peut stocker en outre sous une forme numérique ledit au moins un numéro de document inscrit sur ledit document. Dans ce cas, ledit document peut être déterminé comme étant falsifié si, après relecture dudit numéro de document sous forme numérique depuis ladite mémoire de ladite au moins une puce avec ou sans contacts par ledit lecteur, ledit numéro de document sous forme numérique ainsi relu diffère dudit numéro de document inscrit sur ledit document.

Dans le procédé selon l'invention, la mémoire de ladite puce avec ou sans contacts peut stocker en outre sous forme numérique le nom, et éventuellement les prénoms, et/ou la date de naissance et/ou le lieu de naissance de la personne physique. Si le nom, et éventuellement les prénoms, et/ou la date de naissance et/ou le lieu de naissance de la personne physique sont en outre inscrits sur ledit document, une falsification dudit document peut être détectée si, après relecture dudit nom, et éventuellement desdits prénoms, sous forme numérique et/ou de ladite date de naissance sous forme numérique et/ou dudit lieu de naissance sous forme numérique depuis ladite mémoire de ladite au moins une puce avec ou sans contacts par ledit lecteur, ledit nom, et éventuellement lesdits prénoms, relus diffèrent dudit nom, et éventuellement desdits prénoms, inscrits sur le document et/ou ladite date de naissance diffère de ladite date de naissance inscrite sur ledit document et/ou ledit lieu de naissance diffère dudit lieu de naissance inscrit sur ledit document.

Egalement, dans le procédé de l'invention, ladite mémoire de ladite au moins une puce avec ou sans contacts dudit document peut stocker une ou plusieurs données biométriques et/ou anthropométriques concernant ladite personne physique sous une forme numérique. Dans ce cas, si une ou plusieurs données biométriques et/ou anthropométriques sont inscrites sur ledit document, ledit document peut alors être déterminé comme étant

falsifié si, après relecture desdites une ou plusieurs données biométriques et/ou anthropométriques depuis ladite mémoire de ladite au moins une puce avec ou sans contacts par ledit lecteur, au moins une desdites données biométriques et/ou anthropométriques sous forme numérique ainsi relues diffère de la donnée biométrique et/ou anthropométrique correspondante inscrite sur ledit document.

De plus, l'identité de ladite personne physique peut être déterminée comme étant falsifiée si au moins une desdites données biométriques et/ou anthropométriques sous forme numérique relues depuis ladite mémoire de ladite au moins une puce avec ou sans contacts par ledit lecteur diffère de la donnée biométrique et/ou anthropométrique correspondante relevée sur ladite personne physique.

De même, la mémoire de ladite au moins une puce avec ou sans contacts à mémoire dudit document pourra en outre stocker une date d'expiration pour le document. Si une date d'expiration est en outre inscrite sur ledit document, une falsification dudit document sera déterminée si, après relecture de ladite date sous forme numérique depuis ladite mémoire de ladite au moins une puce avec ou sans contacts par ledit lecteur, ladite date sous forme numérique diffère de ladite date inscrite sur ledit document.

Avantageusement, les données stockées dans ladite mémoire de ladite au moins une puce avec ou sans contacts dudit document seront cryptées.

De préférence, ladite détermination de la falsification ou non dudit document et/ou de la falsification ou non de l'identité de ladite personne physique seront effectuées par un opérateur mettant en œuvre ledit lecteur de puce avec ou sans contacts, ledit lecteur affichant sur un dispositif d'affichage les informations relues depuis ladite mémoire desdites au moins une puce avec ou sans contacts dudit document.

L'invention propose également un système de détection de falsification d'un document délivré à une personne physique, ledit document comportant au moins une photographie conventionnelle permettant d'identifier ladite personne physique, et/ou au moins un numéro de document inscrit permettant d'identifier ledit document de façon unique, et/ou le nom, et éventuellement les prénoms, et/ou la date de naissance et/ou le lieu de naissance de ladite personne physique, et/ou une ou plusieurs données

biométriques et/ou anthropométriques inscrites concernant ladite personne physique, et qui a pour caractéristique le fait qu'il met en œuvre le procédé précédent.

On va maintenant décrire, à titre d'exemple seulement, un mode de réalisation préféré de la présente invention, en se référant au dessin annexé, dans lequel :

la figure 1 est le schéma fonctionnel d'un système de contrôle de l'authenticité d'un document d'identité et de l'identité d'une personne physique, mettant en œuvre le procédé selon l'invention.

En se référant à la figure 1, est représenté un système de contrôle d'identité mettant en œuvre le mode de réalisation préféré du procédé de détection de falsification de document selon l'invention. Dans ce mode de réalisation préféré du procédé de l'invention, le document 2 comporte une puce sans contacts 6, et le système de contrôle d'identité se compose essentiellement d'un lecteur 8 de puce à lecture/écriture sans contacts, ou lecteur 8 de puce sans contacts, constitué principalement d'une bobine d'induction électromagnétique 18, non représentée. En fonctionnement, cette bobine d'induction électromagnétique 18 émet un champ magnétique alternatif de haute fréquence.

La puce à mémoire sans contacts 6 contenue dans le document 2 est essentiellement constituée d'un microprocesseur (non représenté) doté d'une mémoire 7, et d'une inductance 17, non représentées, dont les bornes sont reliées aux bornes d'alimentation du microprocesseur. Lorsque le document 2 est posé sur le, ou approché du, lecteur 8, le champ magnétique alternatif de haute fréquence émis par la bobine d'induction électromagnétique 18 du lecteur 8 passe à travers l'inductance 17, et il provoque, de façon bien connue, l'apparition d'une tension alternative aux bornes de l'inductance 17. Cette tension électrique alternative est alors redressée, et elle alimente le microprocesseur de la puce sans contacts 6.

La transmission d'informations est alors classiquement réalisée par l'émetteur des informations en modulant le champ magnétique de haute fréquence émis par le lecteur 8, mais cette transmission peut aussi être effectuée par tout autre procédé adapté au type de puce avec ou sans contacts 6 utilisé.

Lorsque l'émetteur des informations est le lecteur 8, celui-ci module le champ magnétique alternatif de haute fréquence en modulant la tension alternative aux bornes de la bobine d'induction électromagnétique 18, par exemple, entre deux valeurs prédéterminées. Cette modulation du champ magnétique entre deux valeurs se traduit par une variation correspondante de la tension apparaissant aux bornes de l'inductance 17 de la puce sans contacts 6. La puce sans contacts 6 détecte alors ce changement, qui lui reflète le changement de tension intervenu aux bornes de la bobine d'induction électromagnétique 18, et un élément binaire, ou bit, a donc été ainsi transmis par le lecteur 8 à la puce sans contacts 6.

En répétant autant de fois que nécessaire le procédé qui vient d'être décrit, le lecteur 8 peut donc transmettre un nombre quelconque de bits d'information à la puce sans contacts 6. En conséquence, le lecteur 8 peut ainsi transmettre des instructions ou des données à la puce sans contacts 6 en les encodant en une succession de bits suivant un protocole approprié, et en particulier, l'enregistrement de la mémoire 7 de la puce sans contacts 6 peut être réalisé grâce à ce procédé.

Réciproquement, quand la puce sans contacts 6 souhaite transmettre des informations au lecteur 8, la puce sans contacts 6 module le champ magnétique émis par le lecteur 8 en court-circuitant plus ou moins l'inductance 17. Pour cela, la puce sans contacts 6 fait varier l'impédance présente aux bornes de l'inductance 17, par exemple entre deux valeurs prédéterminées. Cette variation de l'impédance dans le circuit de charge de l'inductance 17 entraîne une variation correspondante du courant électrique dans l'inductance 17, qui, par couplage magnétique, entraîne une variation correspondante du courant électrique circulant dans la bobine d'induction électromagnétique 18. Le lecteur 8 détecte alors cette variation d'intensité dans la bobine d'induction électromagnétique 18, qui reflète le changement d'impédance aux bornes de l'inductance 17 de la puce sans contacts 6, et un bit d'information a donc été transmis par la puce sans contacts 6 au lecteur 8.

En répétant autant de fois que nécessaire le procédé qui vient d'être décrit, la puce sans contacts 6 peut donc transmettre un nombre quelconque de bits d'information au lecteur 8. En conséquence, la puce sans contacts 6

peut ainsi transmettre des données au lecteur 8, en les encodant en une succession de bits suivant un protocole approprié.

Dans le mode de réalisation préféré de l'invention, les données stockées dans la mémoire 7 de la puce sans contacts 6, telles qu'elles seront décrites dans la suite de ce document, sont enregistrées en une seule opération lors de la personnalisation du document 2. La puce sans contacts 6 est alors protégée contre l'écriture pour éviter toute falsification ultérieure des données contenues dans sa mémoire 7.

Cela est réalisé, grâce au procédé d'échange d'informations décrit ci-dessus, en donnant instruction à la puce sans contacts 6 d'interdire, de façon irréversible, toute écriture de données dans la mémoire 7 de la puce sans contacts 6. Une fois cette opération réalisée, l'écriture de données dans la mémoire 7 de la puce sans contacts 6 est définitivement impossible, du fait que l'opération est irréversible.

Les puces utilisées dans la présente invention peuvent être, par exemple, les puces Mirage d'Atmel-Motorola, Mifare 1, 2, Pro de Philips-Mikron, et/ou celles de Micro Electronic Marin, et/ou HyperSecure de la société HyperSecure fondues par SGS-Thomson.

Dans le mode de réalisation préféré de l'invention, le lecteur 8 est complété par un dispositif d'affichage 14 permettant à un opérateur 13 de visualiser les informations relues par le lecteur 8 à partir de la mémoire 7 de la puce sans contacts 6 suivant le procédé précédemment décrit.

Dans le mode de réalisation préférentiel de l'invention, le document 2 comporte une photographie conventionnelle 4 de la personne physique 1 à laquelle a été délivré le document 2. Lors de la personnalisation du document 2, la photographie conventionnelle 4 est numérisée par un opérateur 13 à l'aide d'un dispositif approprié (non représenté), par exemple, un numériseur, un appareil photo numérique, une caméra vidéo numérique, etc., relié au lecteur 8. Cette photographie conventionnelle 4 est stockée dans le lecteur 8 sous la forme d'une photographie numérique 11. Sous le contrôle de l'opérateur 13, le lecteur transfère alors la photographie numérique 11 dans la mémoire 7 de la puce sans contacts 6, en utilisant le procédé décrit plus haut.

Lors de l'utilisation du document 2 par la personne physique 1, par exemple, pour justifier de son identité, un opérateur 13 peut alors vérifier que la photographie conventionnelle 4 n'a pas été falsifiée et/ou que la puce sans contacts 6 n'a pas été remplacée. Pour cela, l'opérateur 13 place le document 2 sur le, ou près du, lecteur 8 et il lui fait relire, à l'aide du procédé décrit plus haut, la photographie numérique 11. Cette dernière est alors affichée par le lecteur 8 sur le dispositif d'affichage 14, et l'opérateur 13 peut alors comparer la photographie conventionnelle présente sur le document 2 avec la photographie numérique 11 affichée sur le dispositif d'affichage 14.

Si les deux photographies diffèrent, alors soit la photographie conventionnelle 4 a été falsifiée, soit la puce sans contacts 6 a été changée. Dans les deux cas, la falsification du document 2 est ainsi détectée par l'opérateur 13.

En outre, l'opérateur 13 peut comparer la photographie numérique 11 affichée sur le dispositif 14 à la personne physique 1. Si la photographie numérique 11 n'est pas celle de la personne 1, alors l'opérateur 13 aura ainsi détecté une usurpation d'identité ou le vol du document 2 par la personne physique 1.

Le procédé de l'invention permet ainsi une triple vérification de l'identité d'une personne physique 1 sur la base de la personne physique 1 elle-même et des deux photographies de cette personne physique 1, l'une de ces photographies étant la photographie conventionnelle 4 sur le document 2, et l'autre étant la photographie sous forme numérique 11 stockée dans la mémoire 7 de la puce sans contacts 6 contenue dans le document 2. Plus précisément, le procédé de l'invention permet à l'opérateur 13 de comparer la photographie conventionnelle 4 présente sur le document 2 à la personne physique 1, de comparer la photographie sous forme numérique 11, telle qu'affichée par le lecteur 8 sur le dispositif d'affichage 14, à la personne physique 1, et de comparer la photographie conventionnelle 4 à la photographie sous forme numérique 11.

Si l'une quelconque de ces comparaisons s'avère négative, alors l'opérateur 13 aura détecté la falsification du document 2 et/ou l'usurpation d'identité

de la personne physique 1. Cette triple possibilité de vérification d'identité n'existe dans aucun système et/ou procédé de la technique antérieure.

Dans le mode de réalisation préféré de l'invention, la mémoire 7 de la puce sans contacts 6 comporte en outre une donnée d'identification, par exemple seize caractères alphanumériques, non modifiable 9, qui est unique parmi toutes les puces avec ou sans contacts 6 fabriquées par le fondeur de la puce avec ou sans contacts 6.

Comme moyen supplémentaire de vérification de l'authenticité du document 2, ce numéro de puce 9 peut être relu, lors de la personnalisation du document 2, depuis la puce sans contacts 6 à l'aide d'un lecteur de puce sans contacts similaire au lecteur 8, et ce numéro 9 peut être inscrit sur le document 2 sous la forme d'un numéro d'identification 10.

Lors de la fabrication du document 2 vierge, la puce sans contacts 6 est intégrée au document 2 par collage, prise en sandwich entre les couches ou les feuillets du document 2, ou par toutes autres techniques appropriées. La puce sans contacts 6 peut également être intégrée dans le document 2 lors de la personnalisation de ce document 2, par collage, par intégration dans le film de sécurité, prise en sandwich entre les couches ou feuillets du documents 2, ou par toutes autres techniques adéquates.

Dans le mode de réalisation préféré de l'invention, les informations propres au titulaire 1 du document 2 sont inscrites à l'aide du lecteur 8 dans la mémoire 7 de la puce sans contacts 6 lors de la personnalisation du document 2.

Lors de l'utilisation du document 2 par la personne physique 1, par exemple, pour justifier de son identité, un opérateur 13 peut vérifier que la puce sans contacts 6 est bien la puce sans contacts 6 d'origine et/ou que le numéro de puce 9 inscrit sur le document 2 n'a pas été falsifié. Pour cela, il pose le document 2 contenant la puce sans contacts 6 sur le, ou près du, lecteur 8, et il fait relire par ce dernier, à l'aide du procédé d'échange d'informations précédemment décrit, le numéro de puce 9 figurant dans la mémoire 7 de la puce sans contacts 6. Ce numéro 9 est alors affiché par le lecteur 8 sur le dispositif d'affichage 14, et l'opérateur 13 peut alors vérifier visuellement la concordance du numéro de puce 9 affiché sur le dispositif d'affichage avec le numéro 10 inscrit sur le document 2.

Le numéro de puce 9 étant unique parmi toutes les puces avec ou sans contacts 6 fabriquées, toute modification du numéro d'identification 10 inscrit sur le document 2 et/ou tout remplacement de la puce sans contacts 6 par une autre puce sans contacts 6 se traduira obligatoirement par une absence de concordance entre le numéro d'identification 6 affiché sur l'écran 14 et le numéro d'identification 10 inscrit sur le document 2, et la falsification du document 2 sera ainsi détectée par l'opérateur 13 effectuant la vérification.

Dans le mode de réalisation préféré de réalisation du procédé selon l'invention, le document 2 comporte en outre un numéro de document 3 unique. Lors de la personnalisation du document 2, ce numéro est inscrit sur le document 2, et il est également enregistré dans la mémoire 7 de la puce sans contacts 6. Pour cela, un opérateur 13 pose le document 2 contenant la puce sans contacts 6 sur un lecteur 8 de puce sans contacts, ou il approche simplement le document 2 du lecteur 8, il indique au lecteur 8 le numéro de document 3 inscrit sur le document 2, et sous le contrôle de l'opérateur 13, le lecteur 8 enregistre le numéro de document 3 sous la forme d'un numéro de document numérique 16 dans la mémoire 7 de la puce sans contacts 6.

Lors de l'utilisation du document 2 par la personne physique 1, par exemple pour justifier de son identité, un opérateur 13 peut alors vérifier que le numéro de document 3 figurant sur le document 2 n'a pas été falsifié, et/ou que la puce sans contacts 6 n'a pas été échangée. Pour cela, l'opérateur 13 pose le document 2 sur le lecteur 8 ou l'en approche, et il fait relire par le lecteur 8 le numéro de document numérique 16 enregistré dans la mémoire 7 de la puce sans contacts 6. Le lecteur 8 affiche alors le numéro 16 sur le dispositif d'affichage 14 et l'opérateur 13 peut alors vérifier visuellement la concordance entre le numéro de document 16 affiché par le dispositif 14 avec le numéro de document 3 inscrit sur le document 2.

La mémoire 7 de la puce sans contacts 6 ayant été protégée contre toute modification lors de la personnalisation du document 2 et le numéro de document 3 étant unique parmi tous les documents 2 fabriqués, toute modification du numéro de document 3 inscrit sur le document 2 et/ou

tout remplacement de la puce sans contacts 6 par une autre puce sans contacts 6 se traduira obligatoirement par une absence de concordance entre le numéro de document 16 affiché sur l'écran 14 et le numéro de document 3 inscrit sur le document 2, et la falsification du document 2 sera ainsi détectée par l'opérateur 13 effectuant la vérification.

De même, dans le mode de réalisation préféré du procédé selon l'invention, la mémoire 7 de la puce sans contacts 6 stocke en outre le nom 19, et éventuellement les prénoms 33, et/ou la date de naissance 20 et/ou le lieu de naissance 21 de la personne physique 1.

Pour cela, lors de la personnalisation du document 2, un opérateur 13 pose le document 2 contenant la puce sans contacts 6 sur le lecteur 8, il introduit le nom 22, et éventuellement les prénoms 34, et/ou la date de naissance 23 et/ou le lieu de naissance 24 de la personne physique 1 inscrits sur ledit document 2 dans le lecteur 8 à l'aide d'un dispositif de saisie tel qu'un clavier 35, et sous le contrôle de l'opérateur 13, le lecteur 8 enregistre sous forme numérique dans la mémoire 7 de la puce sans contacts 6 le nom 19, et éventuellement les prénoms 33, et/ou la date de naissance 20 et/ou le lieu de naissance 21 de la personne physique 1.

Lors de l'utilisation du document 2 par la personne physique 1, par exemple, pour justifier de son identité, un opérateur 13 peut alors vérifier que le numéro de document 3 figurant sur le document 2 n'a pas été falsifié, et/ou que la puce sans contacts 6 n'a pas été échangée. Pour cela, l'opérateur 13 pose le document 2 sur le lecteur 8, et il fait relire par le lecteur 8 le nom 19, et éventuellement les prénoms 33, et/ou la date de naissance 20 et/ou le lieu de naissance 21 enregistrés dans la mémoire 7 de la puce sans contacts 6. Le lecteur 8 affiche alors le numéro 16 sur le dispositif d'affichage 14 et l'opérateur 13 peut alors vérifier visuellement la concordance entre le nom 19, et éventuellement les prénoms 33, et/ou la date de naissance 20 et/ou le lieu de naissance 21 affichés par le dispositif 14 avec le nom 22, et éventuellement les prénoms 34, et/ou la date de naissance 23 et/ou le lieu de naissance 24 inscrits sur le document 2.

Du fait que la mémoire 7 de la puce sans contacts 6 a été protégée contre toute modification des données qu'elle contient lors de la personnalisation du document 2, toute modification du nom 22, et éventuellement des

prénoms 34, et/ou de la date de naissance 23 et/ou du lieu de naissance 24 inscrits sur le document 2 et/ou tout remplacement de la puce sans contacts 6 par une autre puce sans contacts 6 se traduira obligatoirement par une absence de concordance entre le nom 19, et éventuellement les prénoms 33, et/ou la date de naissance 20 et/ou le lieu de naissance 21 affichés sur l'écran 14 et le nom 22, et éventuellement les prénoms 34, et/ou la date de naissance 23 et/ou le lieu de naissance 24 inscrits sur le document 2, et la falsification du document 2 sera ainsi détectée par l'opérateur 13.

Dans le mode de réalisation préféré de l'invention, le document 2 comporte inscrites un certain nombre de données biométriques et/ou anthropométriques 5 concernant la personne physique 1. Lors de la personnalisation du document 2, ces données sont inscrites sous une forme numérique 12 dans la mémoire 7 de la puce sans contacts 6 par l'opérateur 13.

Pour cela, l'opérateur 13 pose le document 2 contenant la puce sans contacts 6 sur le lecteur 8, ou l'approche de celui-ci, et à l'aide d'un dispositif de saisie tel qu'un clavier 35, il entre dans le lecteur 8 ces données biométriques et/ou anthropométriques 5 telles qu'elles apparaissent sur le document 2. Il indique alors au lecteur 8 de transférer ces données dans la mémoire 7 de la puce sans contacts 6. Les données biométriques et/ou anthropométriques sont alors inscrites sous une forme numérique 12 dans la mémoire 7 de la puce sans contacts 6.

Lors de l'utilisation du document 2 par la personne physique 1, par exemple, pour justifier de son identité, un opérateur 13 peut vérifier que les données biométriques et/ou anthropométriques 5 inscrites sur le document 2 n'ont pas été falsifiées et/ou que la puce sans contacts 6 n'a pas été échangée. Pour cela, l'opérateur 13 pose le document 2 contenant la puce sans contacts 6 sur le lecteur 8, et à l'aide du procédé d'échange d'informations décrit plus haut, le lecteur 8, sous le contrôle de l'opérateur 13, relit les données biométriques et/ou anthropométriques 12 contenues dans la mémoire 7 de la puce sans contacts 6, puis le lecteur 8 affiche ces données 12 sur le dispositif d'affichage 14.

L'opérateur 13 peut alors contrôler que les données biométriques et/ou anthropométriques 12 affichées sur le dispositif d'affichage 14 concordent avec les données biométriques et/ou anthropométriques 5 inscrites sur le document 2. La puce sans contacts 6 ayant été protégée contre la modification des données de sa mémoire 7 lors de la personnalisation du document 2, si l'une au moins des données 12 affichées sur le dispositif 14 diffère de la donnée 5 correspondante inscrite sur le document 2, alors soit la donnée 5 inscrite sur le document 2 a été falsifiée, soit la puce sans contacts 6 a été remplacée par une autre.

Dans un cas comme dans l'autre, l'opérateur 13 pourra détecter la falsification du document 2.

Dans le mode de réalisation préféré de l'invention, les données biométriques et/ou anthropométriques 5 ou 12 peuvent comporter, par exemple, la taille, la couleur des yeux, mais aussi une ou plusieurs empreintes digitales de la personne physique 1.

L'opérateur 13 peut alors vérifier que la personne n'a pas usurpé l'identité d'une autre à l'aide d'un document 2 falsifié, en relevant sur la personne physique 1 tout ou partie des données biométriques et/ou anthropométriques correspondant aux données 12 affichées sur le dispositif d'affichage 14, et en vérifiant que les données relevées sur la personne physique 1 correspondent bien aux données 12 affichées.

Dans le cas contraire, l'opérateur 13 aura ainsi détecté, grâce au procédé de l'invention, une usurpation d'identité ou un vol du document 2 par la personne physique 1.

Dans le mode de réalisation préféré de l'invention, la mémoire 7 de la puce sans contacts 6 stocke en outre une date d'expiration pour le document 2. Cette date est enregistrée dans la mémoire 7 de la puce sans contacts 6, de la même manière que les autres informations précédemment décrites, lors de la personnalisation du document 2, c'est-à-dire qu'au moyen d'un dispositif de saisie tel qu'un clavier 35, un opérateur 13 entre dans le lecteur 8 la date d'expiration 25 inscrite sur le document 2 et que, sous son contrôle, le lecteur 8 enregistre cette date d'expiration 25 sous une forme numérique 15 dans la mémoire 7 de la puce sans contacts 6.

Lors de l'utilisation du document 2 par la personne physique 1, par exemple, pour justifier de son identité, un opérateur 13 peut vérifier que la date d'expiration inscrite sur le document 2 n'a pas été falsifiée et/ou que la puce sans contacts 6 n'a pas été échangée. Pour cela, l'opérateur 13 pose le document 2 contenant la puce sans contacts 6 sur le lecteur 8, ou l'en approche, et à l'aide du procédé d'échange d'informations décrit plus haut, le lecteur 8, sous le contrôle de l'opérateur 13, relit la date d'expiration sous forme numérique 15 enregistrée dans la mémoire 7 de la puce sans contacts 6, puis le lecteur 8 affiche cette date 15 sur le dispositif d'affichage 14.

L'opérateur 13 peut alors contrôler que la date 15 affichée sur le dispositif d'affichage 14 concorde avec la date 25 inscrite sur le document 2. La puce sans contacts ayant été protégée contre l'écriture lors de la personnalisation du document 2, si la date 15 affichée sur le dispositif 14 diffère de la date 25 inscrite sur le document 2, alors soit la date 25 inscrite sur le document 2 a été falsifiée, soit la puce sans contacts 6 a été remplacée par une autre.

Dans les deux cas, l'opérateur 13 pourra alors détecter la falsification du document 2.

Dans le mode de réalisation préféré de l'invention, les données stockées dans la mémoire 7 de la puce sans contacts 6 sont cryptées à l'aide d'un procédé tenu secret, de façon à ce que, même en cas d'une démocratisation de la technologie permettant à un faussaire de réaliser de fausses puce sans contacts 6, il ne soit pas possible à un faussaire de crypter les données de façon appropriée dans une puce sans contacts 6 contrefaite.

De préférence, le procédé secret ci-dessus sera typiquement implémenté dans le lecteur 8, et/ou dans la puce avec ou sans contacts 6, d'une façon telle que le vol d'un lecteur 8, ou même la connaissance du procédé de décryptage contenu dans le lecteur 8, ne puisse permettre de connaître le procédé d'encryptage nécessaire pour réaliser une puce sans contacts 6 qui puisse être relue sans erreur par le lecteur 8.

Dans ce qui précède, les vérifications concernant la validité d'un document 2 et/ou le contrôle de l'identité d'une personne physique 1 ont été faites, pour la simplicité de l'exposé, en supposant l'intervention d'un opérateur 13. Toutefois, des techniques appropriées ne faisant pas appel à un

opérateur humain 13 pourront être utilisées chaque fois que cela présentera un intérêt en pratique. En particulier, la lecture des informations inscrites sur le document 2 par un opérateur 13 pourra être remplacée par une reconnaissance optique des caractères inscrits sur le document 2 par un système informatisé. De même, certaines données biométriques et/ou anthropométriques 5 ou 12 telles la taille, la couleur des yeux, et/ou des empreintes digitales pourront être obtenues à l'aide d'un dispositif automatisé ne faisant pas appel à un opérateur humain 13.

Ainsi, un procédé de détection de falsification d'un document 2 a été décrit, qui permet de détecter un grand nombre de falsifications des inscriptions figurant sur un document 2, grâce à l'intégration dans le document 2 d'une puce avec ou sans contacts 6. Ce procédé permet de pallier les insuffisances de documents 2 actuels tels que passeports, visas, cartes d'identité nationales, permis de conduire et/ou de travail, etc., dont la falsification ne présente plus guère de difficulté pour un faussaire expérimenté.

Entre autres, le procédé de l'invention offre une possibilité de triple vérification de l'identité d'une personne physique 1, en permettant en quelques secondes la comparaison d'une photographie conventionnelle 4 présente sur le document 2 à la personne physique 1, la comparaison d'une photographie sous forme numérique 11 stockée dans la mémoire 7 de la puce sans contacts 6 dans le document 2 à la personne physique 1, et la comparaison de la photographie conventionnelle 4 à la photographie sous forme numérique 11. Associée aux autres contrôles décrits ci-dessus, cette triple possibilité permet de détecter, dans la technique actuelle, toute forme de falsification du document 2 et/ou d'usurpation d'identité de la personne physique 1. Cette possibilité n'est offerte par aucun procédé et/ou système de la technique antérieure.

L'efficacité du procédé de l'invention est garantie par l'impossibilité, dans l'état actuel de la technique, de falsifier une puce sans contacts 6 existante, du fait de la protection contre l'écriture réalisée au moment de sa personnalisation. De même, l'utilisation d'un procédé de cryptage secret permet d'interdire à un faussaire la réalisation d'une puce sans contacts 6 valide à partir d'une puce sans contacts vierge non programmée.

Ces caractéristiques font que le procédé de l'invention est susceptible d'une très large application dans des domaines aussi variés que le contrôle d'identité des ressortissants d'un état, ou l'accès à des zones protégées telles que des zones militaires ou des zones civiles sensibles telles que le nucléaire, les industries de l'armement et les centres de recherche de tout type, et d'une façon générale, dans tous les domaines où l'authentification de l'identité d'une personne physique 1 est primordiale.

REVENDICATIONS

1. Procédé de détection de falsification d'un document (2) délivré à une personne physique (1), ledit document (2) comportant au moins une photographie conventionnelle (4) permettant d'identifier ladite personne physique (1), et/ou au moins un numéro de document (3) inscrit permettant d'identifier ledit document (2) de façon unique, et/ou le nom (19), et éventuellement les prénoms (33), et/ou la date de naissance (20) et/ou le lieu de naissance (21) de la personne physique (1), et/ou une ou plusieurs données biométriques et/ou anthropométriques (5) inscrites concernant ladite personne physique (1), caractérisé par le fait que ledit document (2) délivré à ladite personne physique (1) comporte en outre au moins une puce avec ou sans contacts (6) à lecture/écriture avec ou sans contacts, ou puce avec ou sans contacts (6), ladite au moins une puce avec ou sans contacts (6) comportant une mémoire (7), les données contenues dans ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) pouvant être lues et/ou écrites par un lecteur (8) de puce avec ou sans contacts.

2. Procédé selon la revendication 1, dans lequel ladite puce avec ou sans contacts (6) comporte en outre au moins un microprocesseur (30).

3. Procédé selon la revendication 1 ou 2, dans lequel ladite puce avec ou sans contacts (6) comporte en outre au moins un microcontrôleur (31).

4. Procédé selon l'une des revendications 1 à 3, dans lequel ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) dudit document ~~(2) stocke en outre une donnée d'identification non modifiable (9) identifiant~~ de façon unique ladite puce avec ou sans contacts (6).

5. Procédé selon la revendication 4, dans lequel ladite donnée non ~~modifiable (9) dans la mémoire (7) est inscrite sous une forme appropriée~~

(10) sur ledit document (2) et dans lequel ledit document (2) est déterminé comme étant falsifié si, après relecture de ladite donnée (9) depuis ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) par ledit lecteur (8), ladite donnée (9) ainsi relue diffère de ladite donnée (10) inscrite sur ledit document (2).

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel lesdites données contenues dans ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) dudit document (2) sont protégées contre toute modification postérieure à l'enregistrement initial desdites données.

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel une ou plusieurs photographies sous forme numérique (11) de ladite personne physique (1) sont en outre stockées dans la mémoire (7) de ladite au moins une puce avec ou sans contacts (6) dudit document (2).

8. Procédé selon la revendication 7, dans lequel ledit document (2) comporte en outre une ou plusieurs photographies conventionnelles (4) de ladite personne physique (1) et dans lequel ledit document (2) est déterminé comme étant falsifié si, après relecture desdites une ou plusieurs photographies sous forme numérique (11) depuis ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) par ledit lecteur (8), au moins une photographie sous forme numérique (11) ainsi relue diffère de la photographie conventionnelle (4) correspondante sur ledit document (2).

9. Procédé selon la revendication 7 ou 8, dans lequel l'identité de ladite ~~personne physique (1) est déterminée comme étant falsifiée si,~~ après relecture desdites une ou plusieurs photographies sous forme numérique (11) depuis ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) par ledit lecteur (8), au moins une photographie sous forme numérique (11) ainsi relue ne correspond pas à ladite personne physique (1).

10. Procédé selon l'une quelconque des revendications précédentes, dans lequel au moins un numéro de document (3) est inscrit sur ledit document (2) et dans lequel ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) dudit document (2) stocke en outre sous une forme numérique (16) ledit au moins un numéro de document (3) inscrit sur le document (2).

11. Procédé selon la revendication 10, dans lequel ledit document (2) est déterminé comme étant falsifié si, après relecture dudit numéro de document (3) sous forme numérique (16) depuis ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) par ledit lecteur (8), ledit numéro de document (3) sous forme numérique (16) ainsi relu diffère dudit numéro de document (3) inscrit sur ledit document (2).

12. Procédé selon l'une quelconque des revendications précédentes, dans lequel la mémoire (7) de ladite puce avec ou sans contacts (6) stocke en outre sous forme numérique le nom (19), et éventuellement les prénoms (33), et/ou la date de naissance (20) et/ou le lieu de naissance (21) de la personne physique (1).

13. Procédé selon la revendication 12, dans lequel le nom (22), et éventuellement les prénoms (34), et/ou la date de naissance (23) et/ou le lieu de naissance (24) de la personne physique (1) sont inscrits sur ledit document (2) et dans lequel une falsification dudit document (2) est détectée si, après relecture dudit nom sous forme numérique (19), et éventuellement desdits prénoms (33) sous forme numérique, et/ou de ladite date de naissance sous forme numérique (20) et/ou dudit lieu de naissance sous forme numérique (21) depuis ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) par ledit lecteur (8), ledit nom (19), et éventuellement lesdits prénoms (33), relus diffèrent dudit nom (22), et éventuellement desdits prénoms (34), inscrits sur ledit document (2) et/ou ladite date de naissance (20) relue diffère de ladite date de naissance (23)

inscrite sur ledit document (2) et/ou ledit lieu de naissance (21) relu diffère dudit lieu de naissance (24) inscrit sur ledit document (2).

14. Procédé selon l'une quelconque des revendications précédentes, dans lequel ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) dudit document (2) stocke une ou plusieurs données biométriques et/ou anthropométriques concernant ladite personne physique (1) sous une forme numérique (12).

15. Procédé selon la revendication 14, dans lequel une ou plusieurs données biométriques et/ou anthropométriques (5) sont inscrites sur ledit document (2) et dans lequel ledit document (2) est déterminé comme étant falsifié si, après relecture desdites une ou plusieurs données biométriques et/ou anthropométriques sous forme numérique (12) depuis ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) par ledit lecteur (8), au moins une desdites données biométriques et/ou anthropométriques sous forme numérique (12) ainsi relues diffère de la donnée biométrique et/ou anthropométrique (5) correspondante inscrite sur ledit document (2).

16. Procédé selon la revendication 14 ou 15, dans lequel l'identité de ladite personne physique (1) est déterminée comme étant falsifiée si, après relecture desdites une ou plusieurs données biométriques et/ou anthropométriques sous forme numérique (12) depuis ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) par ledit lecteur (8), au moins une desdites données biométriques et/ou anthropométriques sous forme numérique (12) ainsi relues diffère de la donnée biométrique et/ou anthropométrique correspondante relevée sur ladite personne physique (1).

17. Procédé selon l'une quelconque des revendications précédentes, dans lequel la mémoire (7) de ladite au moins une puce avec ou sans contacts (6) dudit document (2) stocke en outre sous forme numérique une date d'expiration (15) pour le document (2).

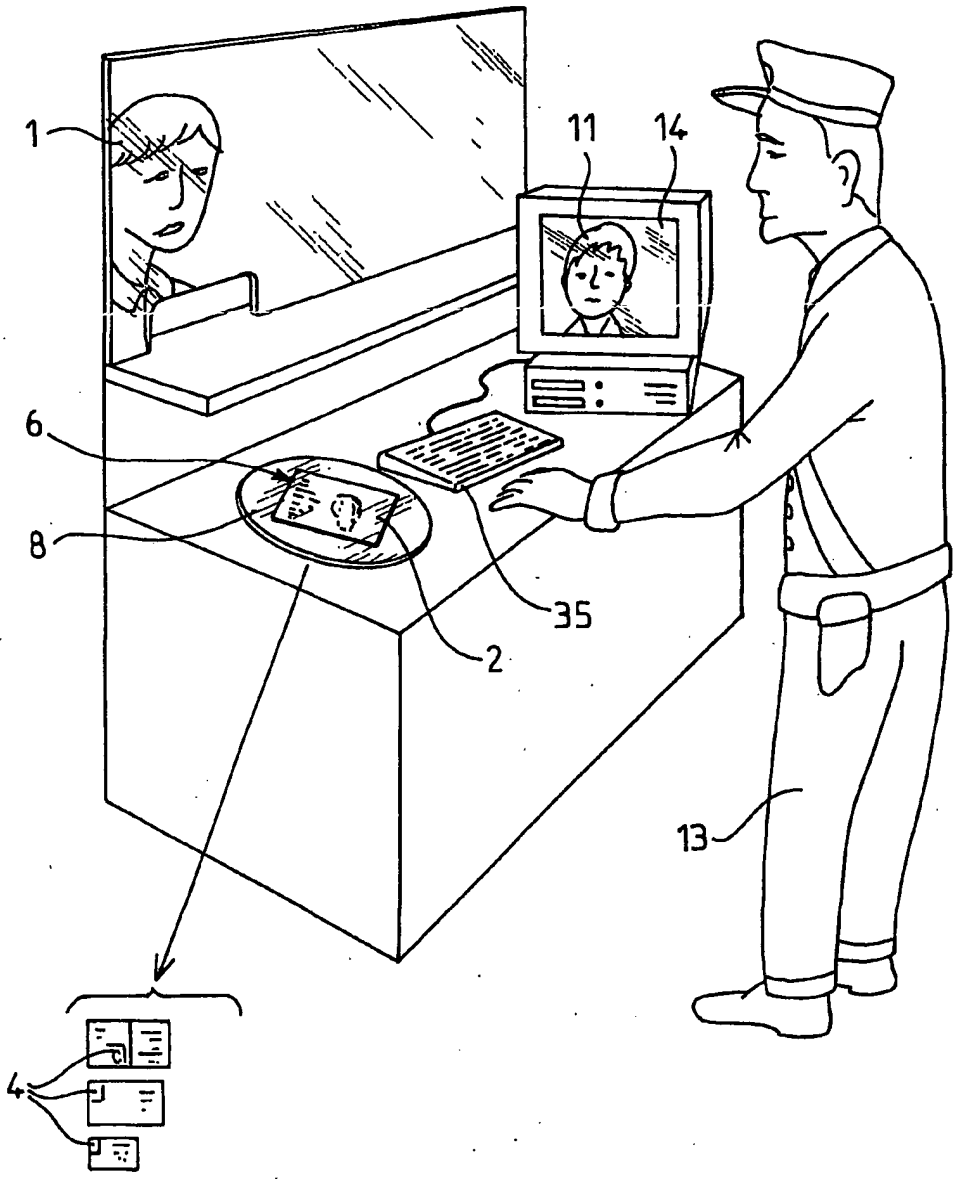
18. Procédé selon la revendication 17, dans lequel une date d'expiration (25) est inscrite sur ledit document (2) et dans lequel une falsification dudit document (2) est déterminée si, après relecture de ladite date sous forme numérique (15) depuis ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) par ledit lecteur (8), ladite date sous forme numérique (15) diffère de ladite date (25) inscrite sur ledit document (2).

19. Procédé selon l'une quelconque des revendications précédentes, dans lequel les données stockées dans ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) dudit document (2) sont cryptées.

20. Procédé selon l'une quelconque des revendications précédentes, dans lequel ladite détermination de la falsification ou non dudit document (2) et/ou de la falsification ou non de l'identité de ladite personne physique (1) sont effectuées par un opérateur (13) mettant en œuvre ledit lecteur (8) de puce avec ou sans contacts, ledit lecteur (8) affichant sur un dispositif d'affichage (14) les informations relues depuis ladite mémoire (7) de ladite au moins une puce avec ou sans contacts (6) dudit document (2).

21. Système de détection de falsification d'un document (2) délivré à une personne physique (1), ledit document (2) comportant au moins une photographie conventionnelle (4) permettant d'identifier ladite personne physique (1), et/ou au moins un numéro de document (3) inscrit permettant d'identifier ledit document (2) de façon unique, et/ou le nom (19) et éventuellement les prénoms (33), et/ou la date de naissance (20) et/ou le lieu de naissance (21) de la personne physique (1), et/ou une ou plusieurs données biométriques et/ou anthropométriques (5) inscrites concernant ladite personne physique (1), caractérisé par le fait qu'il met en œuvre le procédé selon l'une quelconque des revendications précédentes.

1/1



INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 00/02462

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/08 G07F7/08 G06K19/07 B42D15/10 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G07F B42D G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 776 153 A (ORDICAM RECH ET DEV) 17 September 1999 (1999-09-17) the whole document ---	1-4,6-8, 12-15, 19-21
X	US 5 742 685 A (BERSON WILLIAM ET AL) 21 April 1998 (1998-04-21) column 3, line 43 -column 5, line 4 figures 1-3 ---	1-4,7-9, 19-21
X	US 5 913 542 A (BELUCCI BARRY ET AL) 22 June 1999 (1999-06-22) column 3, line 14 -column 4, line 1 figure 1 --- -/--	1,7,8, 12,13, 19-21

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 July 2001	19/07/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	de Ronde, J.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Ir nal Application No
PCT/FR 00/02462

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	DE 199 06 388 A (BUNDESDRUCKEREI GMBH) 24 August 2000 (2000-08-24) the whole document	1-3, 14-16, 19-21

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 00/02462

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2776153 A	17-09-1999	WO 0120564 A	22-03-2001
		AU 5627799 A	17-04-2001
US 5742685 A	21-04-1998	NONE	
US 5913542 A	22-06-1999	US 5505494 A	09-04-1996
		AT 193490 T	15-06-2000
		CA 2171450 A	23-03-1995
		DE 69424792 D	06-07-2000
		DK 719220 T	16-10-2000
		EP 0719220 A	03-07-1996
		ES 2149283 T	01-11-2000
		GR 3034318 T	29-12-2000
		PT 719220 T	30-11-2000
		WO 9507824 A	23-03-1995
		US 5635012 A	03-06-1997
DE 19906388 A	24-08-2000	WO 0049583 A	24-08-2000

RAPPORT DE RECHERCHE INTERNATIONALE

C Internationale No
PCT/FR 00/02462

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06K19/08 G07F7/08 G06K19/07 B42D15/10 G07C9/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06K G07F B42D G07C

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	FR 2 776 153 A (ORDICAM RECH ET DEV) 17 septembre 1999 (1999-09-17) le document en entier	1-4,6-8, 12-15, 19-21
X	US 5 742 685 A (BERSON WILLIAM ET AL) 21 avril 1998 (1998-04-21) colonne 3, ligne 43 -colonne 5, ligne 4 figures 1-3	1-4,7-9, 19-21
X	US 5 913 542 A (BELUCCI BARRY ET AL) 22 juin 1999 (1999-06-22) colonne 3, ligne 14 -colonne 4, ligne 1 figure 1	1,7,8, 12,13, 19-21

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
12 juillet 2001	19/07/2001

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé
de Ronde, J.

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Internationale No
PCT/FR 00/02462

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
X	DE 199 06 388 A (BUNDESDRUCKEREI GMBH) 24 août 2000 (2000-08-24) le document en entier	1-3, 14-16, 19-21

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

[ ] Internationale No
PCT/FR 00/02462

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
FR 2776153	A	17-09-1999	WO	0120564 A	22-03-2001
			AU	5627799 A	17-04-2001
US 5742685	A	21-04-1998	AUCUN		
US 5913542	A	22-06-1999	US	5505494 A	09-04-1996
			AT	193490 T	15-06-2000
			CA	2171450 A	23-03-1995
			DE	69424792 D	06-07-2000
			DK	719220 T	16-10-2000
			EP	0719220 A	03-07-1996
			ES	2149283 T	01-11-2000
			GR	3034318 T	29-12-2000
			PT	719220 T	30-11-2000
			WO	9507824 A	23-03-1995
			US	5635012 A	03-06-1997
DE 19906388	A	24-08-2000	WO	0049583 A	24-08-2000